Étude Comparative

Bien sûr, voici un tableau comparatif simplifié basé sur les meilleures caractéristiques de chaque solution :

| **Critères / Solutions** | Security Onion | OSSEC | Snort | Sagan |
| --- | --- | --- | --- | --- |
| Description | Plateforme complète pour la détection d'intrusions (IDS/IPS) intégrant divers outils de sécurité. | Solution de sécurité complète pour la détection d'intrusions multiplateformes. | Système de détection d'intrusions (IDS) réseau open source. | Système IDS/IPS open source, excelle dans la corrélation d'événements pour une détection avancée des menaces. |
| Avantages | - Intégration puissante d'outils  - Interface utilisateur conviviale  - Support actif de la communauté (GitHub : +300 Followers/Reddit : +4k/Youtube : +10k) | - Flexibilité et gratuité open source  - Corrélation avancée des événements  - Réponse automatisée aux menaces  -Forum actif ( 29979 post & 5680 topic ) | - Base de signatures étendue  - Configurabilité élevée  - Gratuit et open source  - Communauté active (blog) | -Corrélation performante -Architecture modulaire extensible  -Gestion avancée des logiciels malveillants  -Soutien actif de la communauté |
| Inconvénients | - Configuration nécessitant de l'expertise  - Exigences en ressources matérielles | - Courbe d'apprentissage prononcée  - Personnalisation complexe | - Configuration avancée nécessitant de l'expérience  - Dépendance aux signatures  - Complexité pour les règles personnalisées | - Configuration complexe pour les débutants  - Interface utilisateur moins intuitive  - Exigences élevées en ressources matérielles  - Documentation limitée. |